Quantitative Risk Assessment System Overview

March, 2004
College Park, Maryland

Introduction to Risk Analysis

- Determine potential undesirable consequences associated with use of systems and processes
- Identify ways that such consequences could materialize
- Estimate the likelihood (e.g., probability) of such events
- Provide input to decision makers on optimal strategies to reduce the levels of risk

Definition of Risk

- Risk is usually associated with the uncertainty and undesirability of a potential situation or event
- In order to have a risk situation, both elements must be present

Risk = Uncertainty and Undesirability

Risk = Likelihood and Severity

Risk Assessment

- Risk assessment is the process of providing answer to four basic questions:

    1. What can go wrong?
    2. What are the consequences?
    3. How frequently might they happen?
    4. How confident are we about our answer to the above questions?

- Answering these questions could be simple or require a significant amount of analysis and modeling.

Risk Management

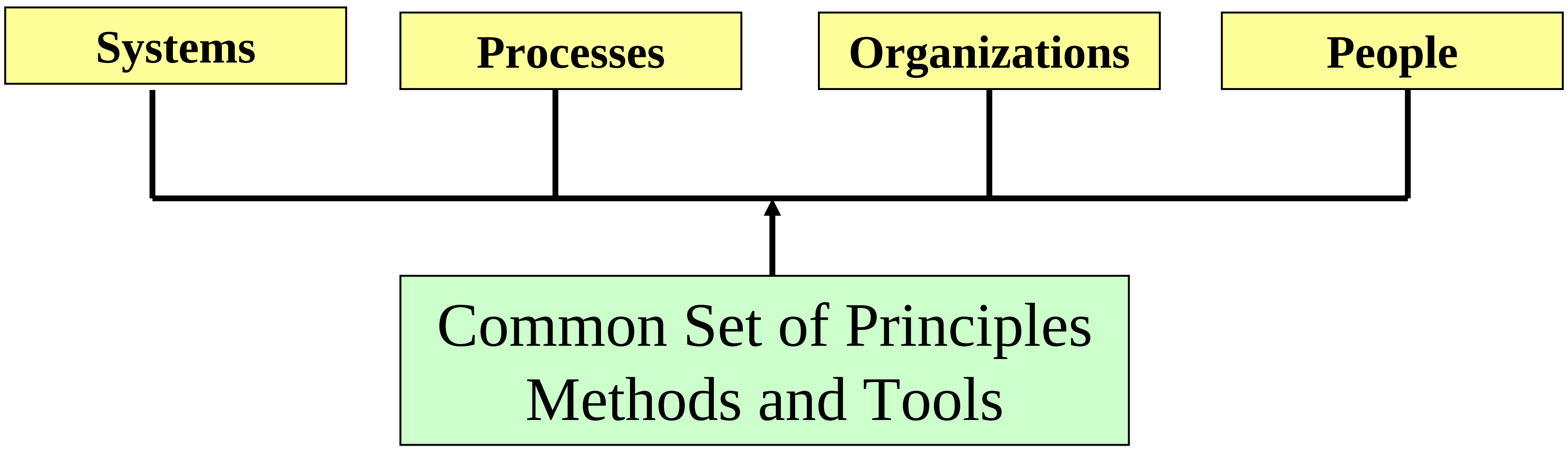
Managing risk requires answers to the following questions:

1. What can be done:
   - to prevent/avoid risk?
   - to mitigate risk?
   - to detect/notify of risk?

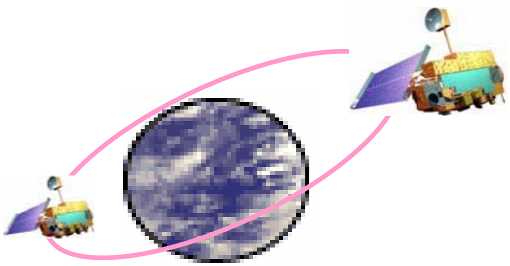
2. How much will it cost?

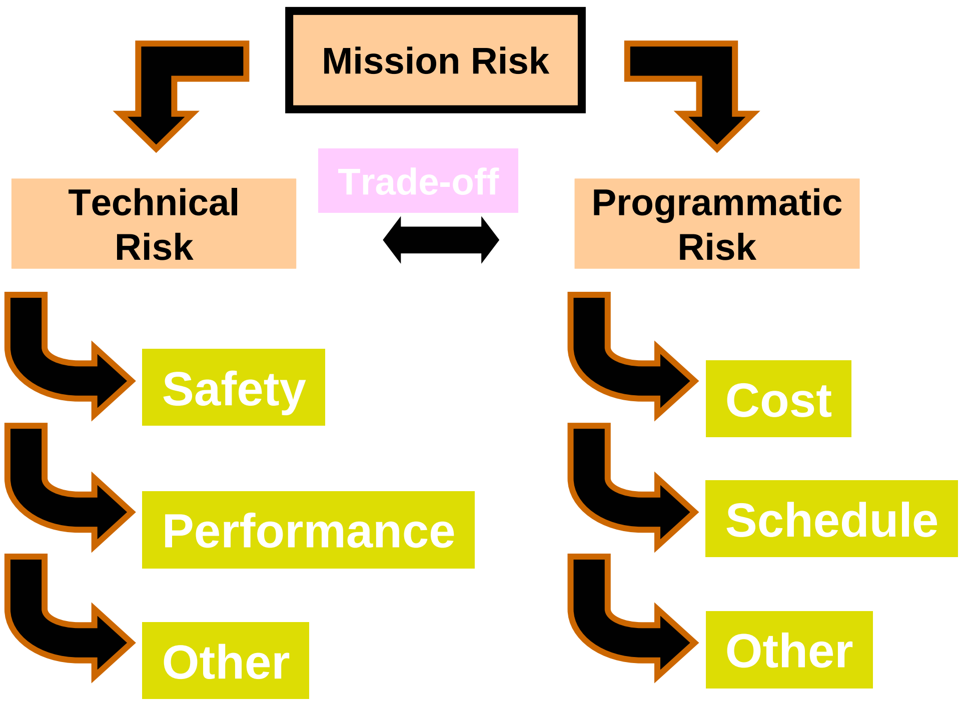
3. How efficient is it?

Domains of Application



NASA Risk Management Perspective





QRAS Overview

- Quantitative Risk Assessment System (QRAS)
- A software tool for quantitative risk assessment
- QRAS can be used to:
  - Build and Manage a Risk Model
  - Develop a Quantitative Measure of Risk
  - Answer Risk Management Questions

A Brief History

- Development at UMD Commissioned by NASA in 1996
- Version 1 and completed in 1997
- An application to Space Shuttle PRA was completed in 1997 by various NASA centers
- In 2001 Version 1.7 was released for beta testing by NASA. Space Station PRA model was used for that purpose
- In 2003 NASA and UMD gave commercialization license to Item Software

QRAS Design Philosophy

- Address large scale PRA models needs such as NASA space shuttle model
- Use leading edge, proven, technology in risk analysis
- Bridge the communication and skill gap between risk analysts, system designers, operators, and decision makers

Classical PRA Methodology

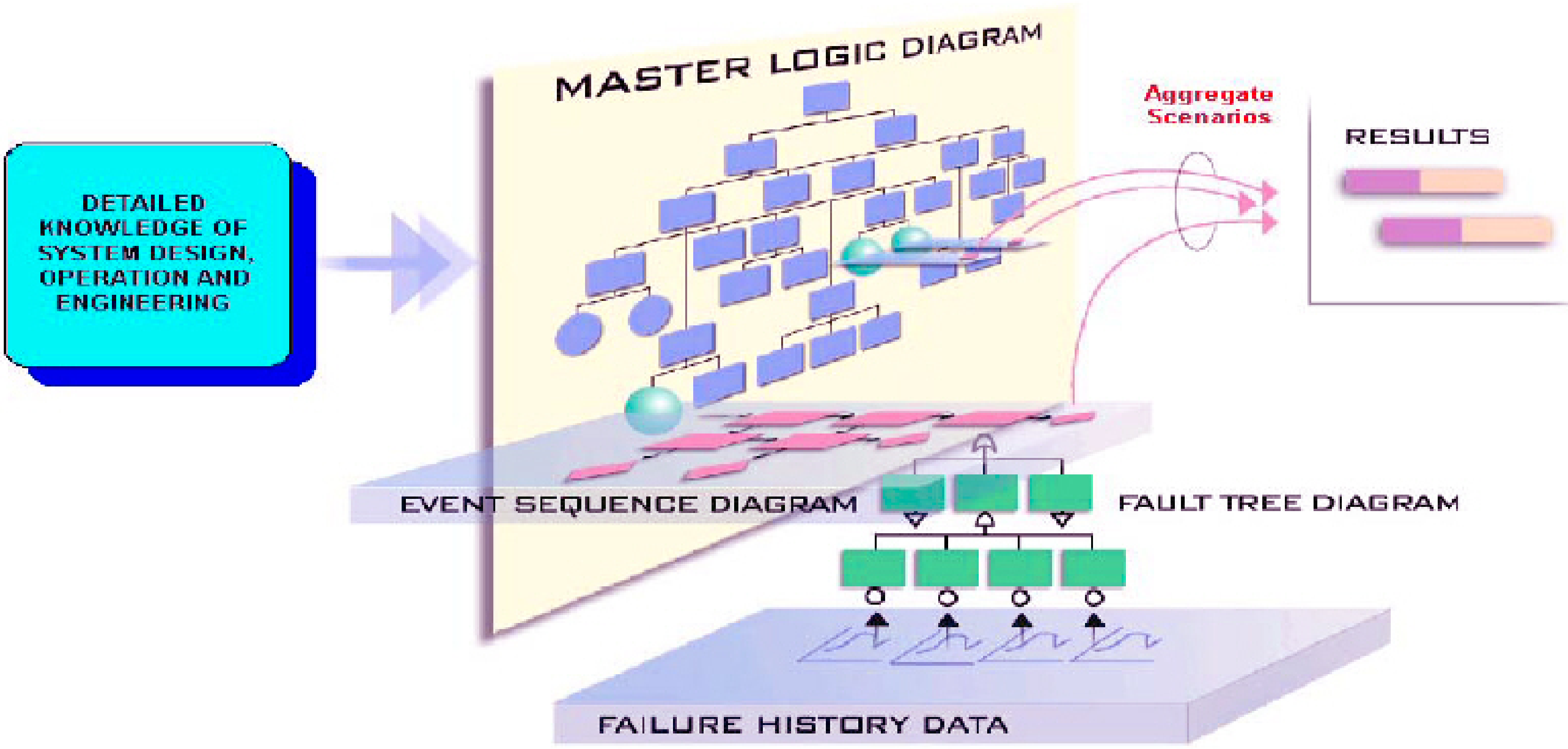
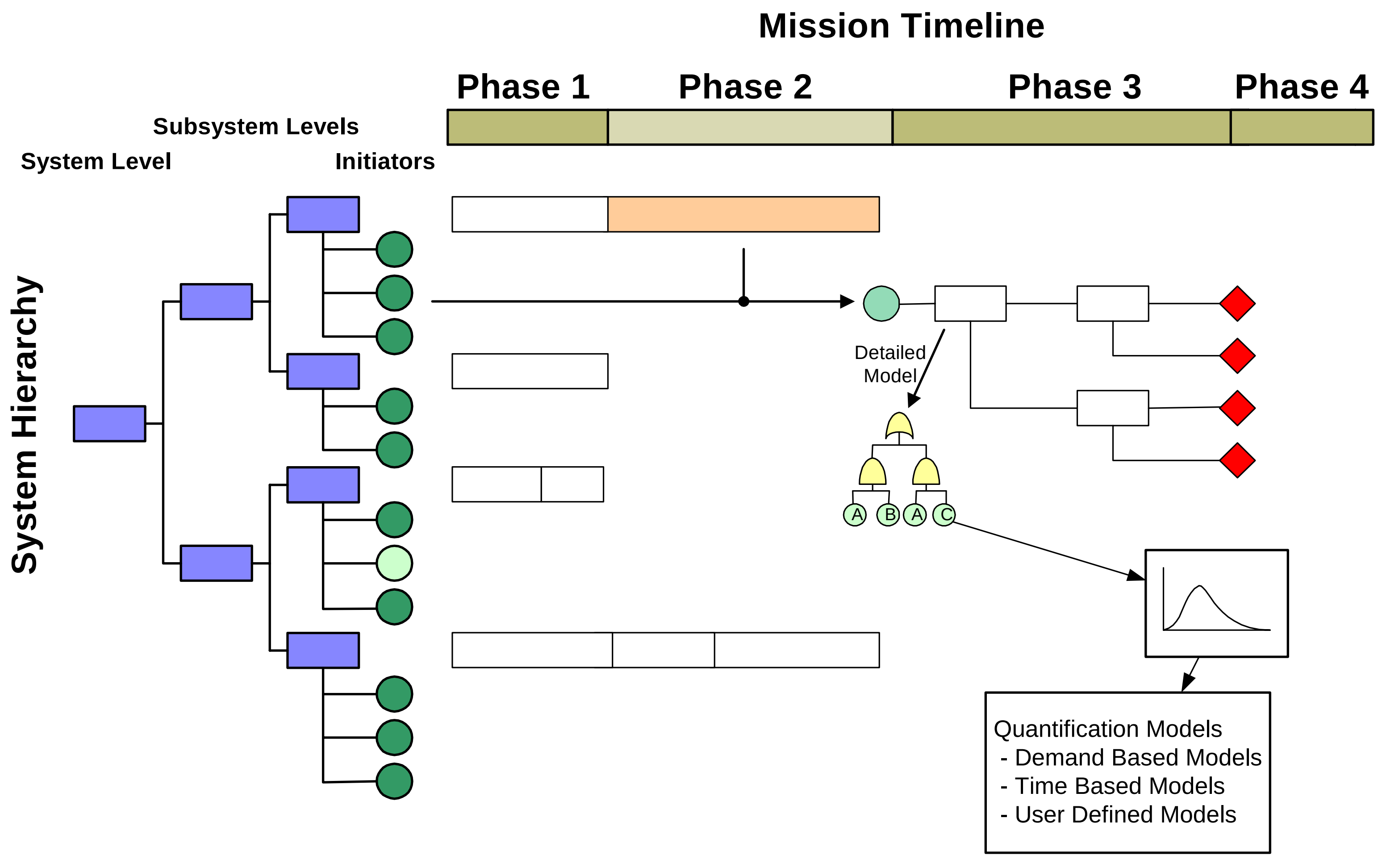


Figure originally composed by Futron Corp.

PRA Model Building with QRAS



QRAS Analysis Capabilities

- Risk Quantification, Point Estimate and Uncertainty
- Automatic Generation of Event Trees from Event Sequence Diagrams
- Risk Contributor and "What-if" Analyses
- Comprehensive Merge Capability

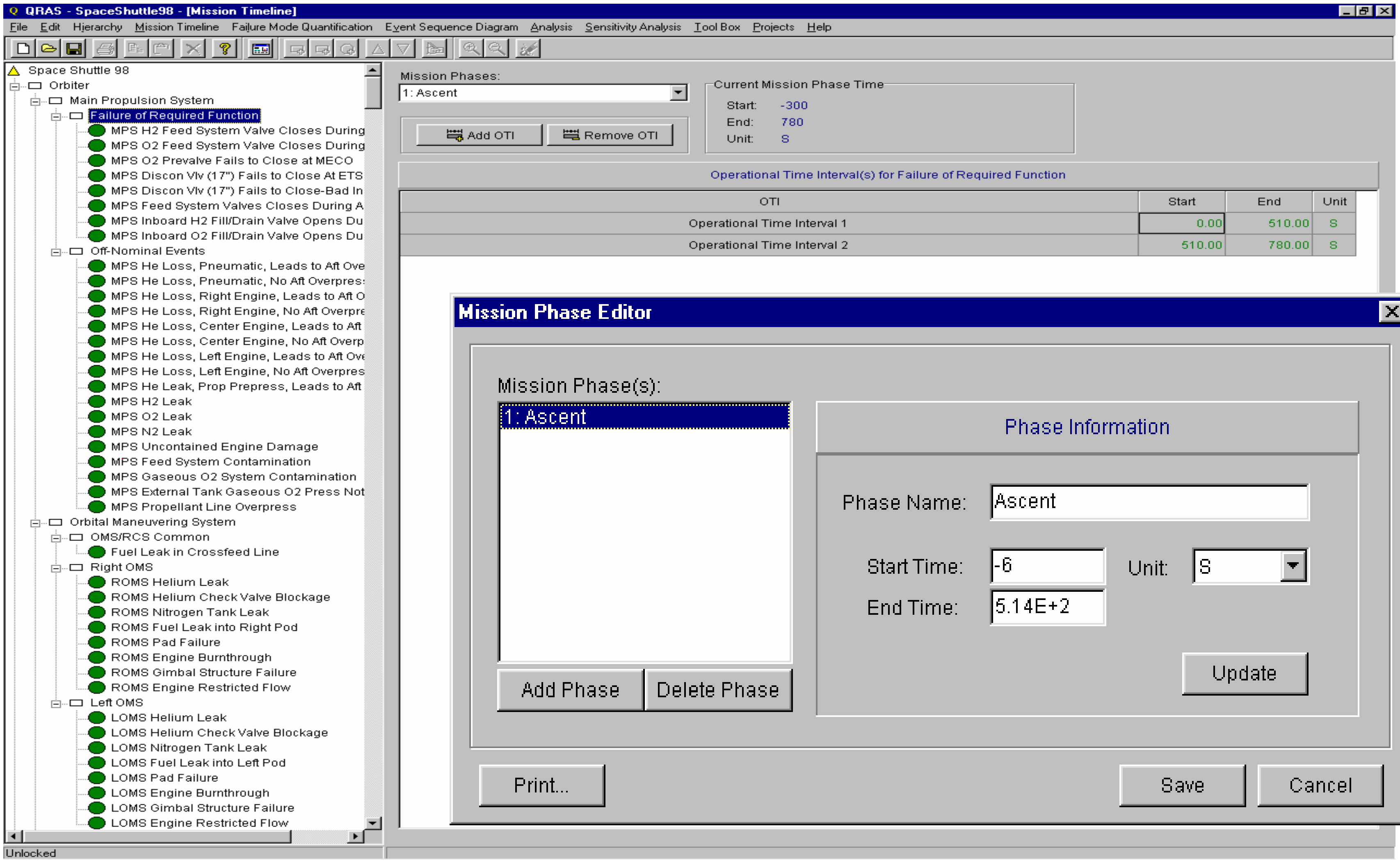
Creating System Hierarchy

- The System Hierarchy Manager is used to breakdown the system into various levels.
  - Root Level: Represents the system itself.
  - Elements: First level of decomposition. Represents high level functions or collection of subsystems.
  - Subsystems: Further detailed level. User can have any level of indentation defined by subsystems.

Creating System Hierarchy cont…

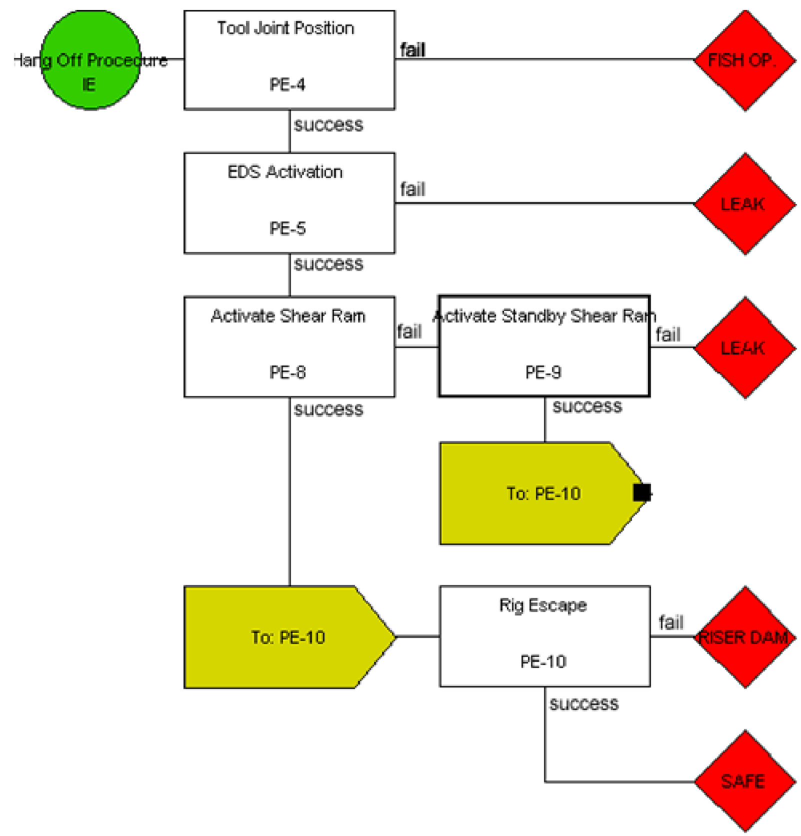
– Initiating Events: Represent the lowest level of hierarchy. These are the failure modes of equipments, hazards associated with equipments or effects of external events (like fire etc).

Mission Timelines and OTIs



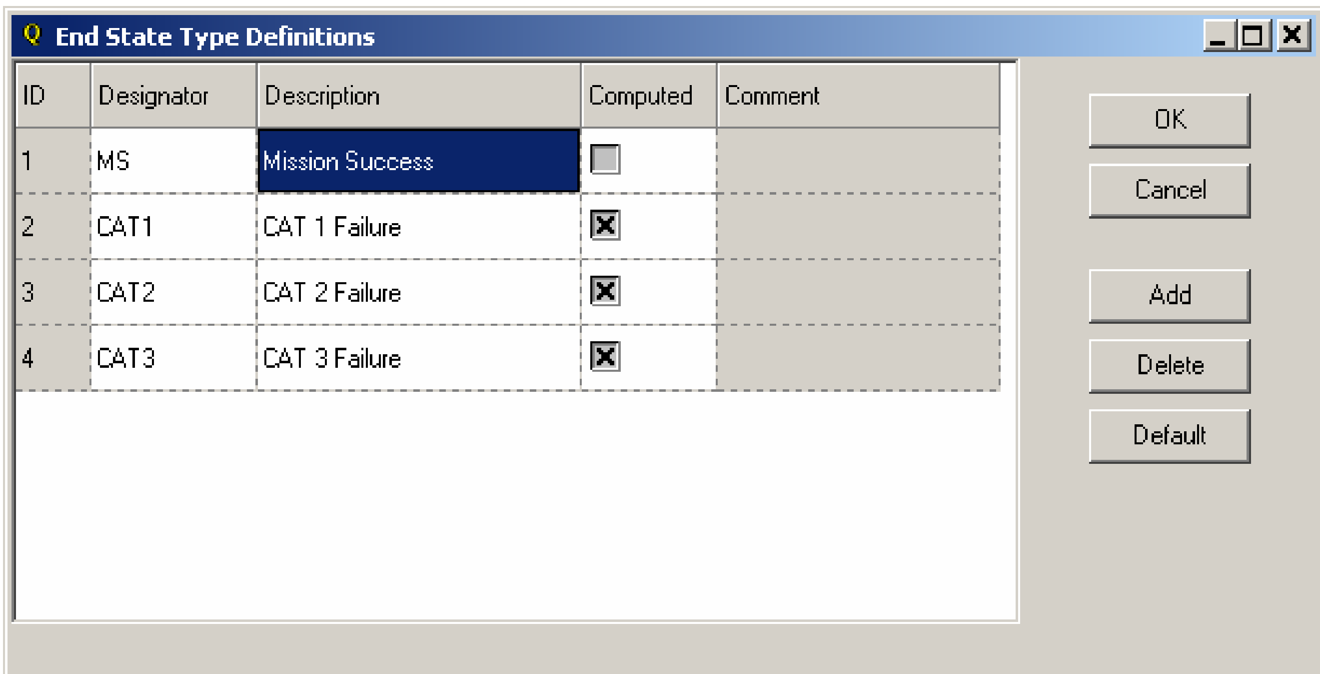
Event Sequence Diagram

- Initiators are starting point of risk scenarios
  - E.g. maintenance operation
- Pivotal event are major events describing determining outcome
  - E.g. procedural steps
- End states are used to classify outcome of scenarios



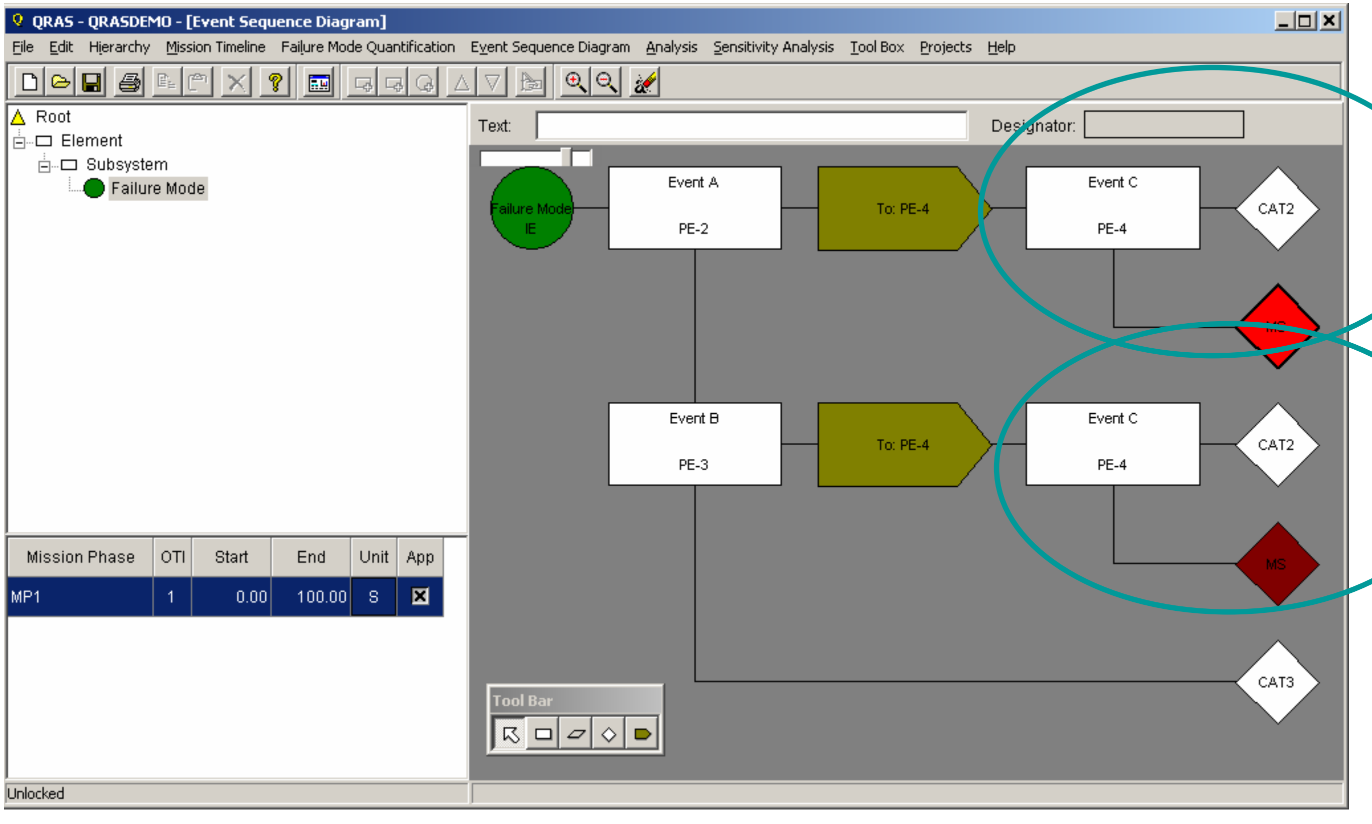
User-Definable End States

- Number and type of end states can be tailored to specific problem needs



ESD Transfer Points

- ESD portions can be reused when scenarios can be combined

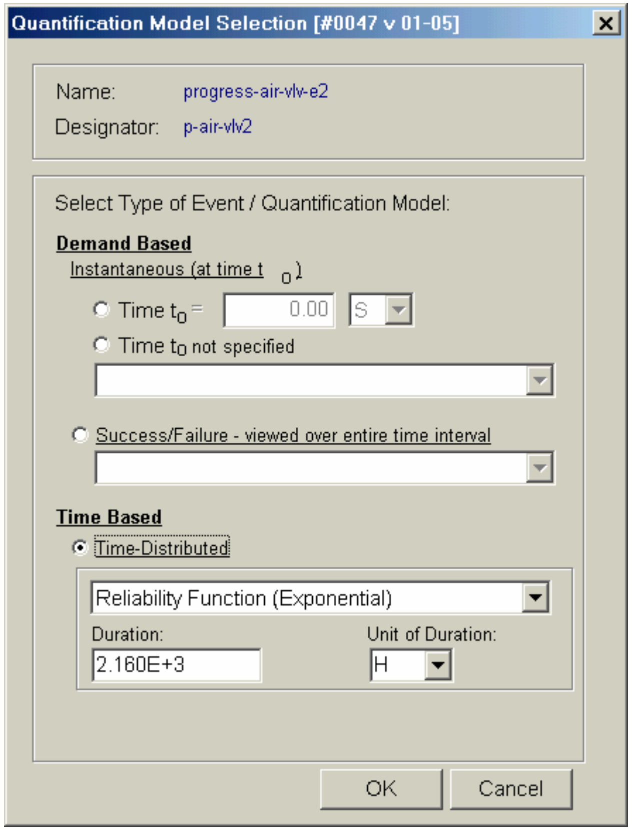


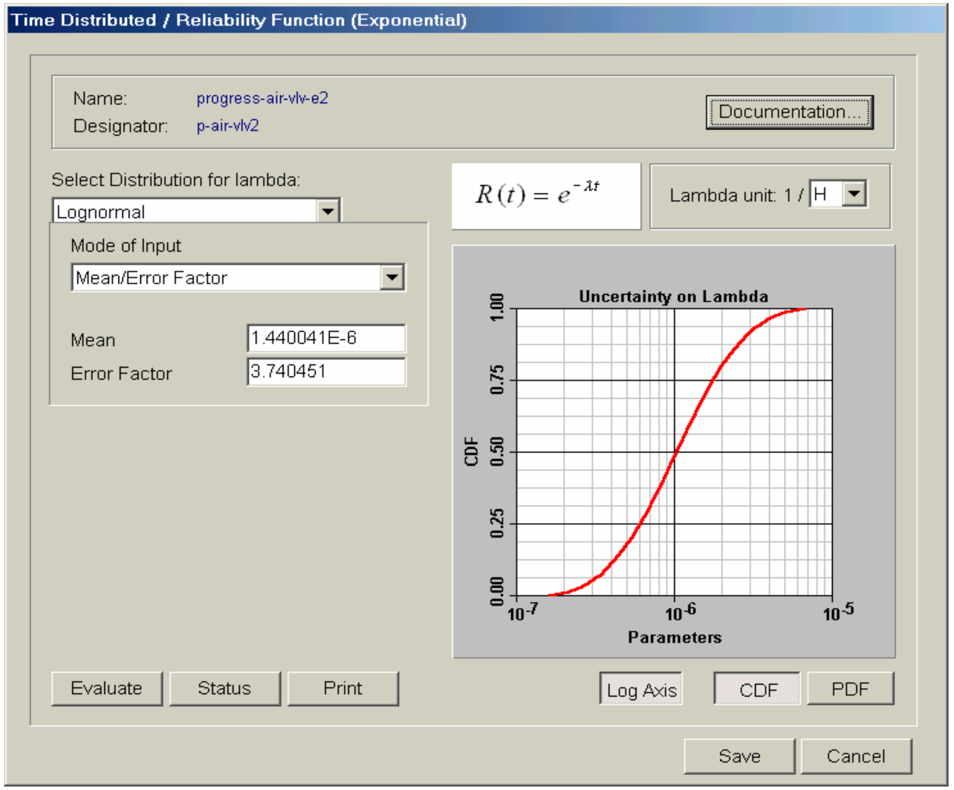
Assigning Quantification Models

- Type of the quantification model can be:
  - Instantaneous
  - Success/Failure Type
  - Time Based
  - Fault Tree

Quantification of Events

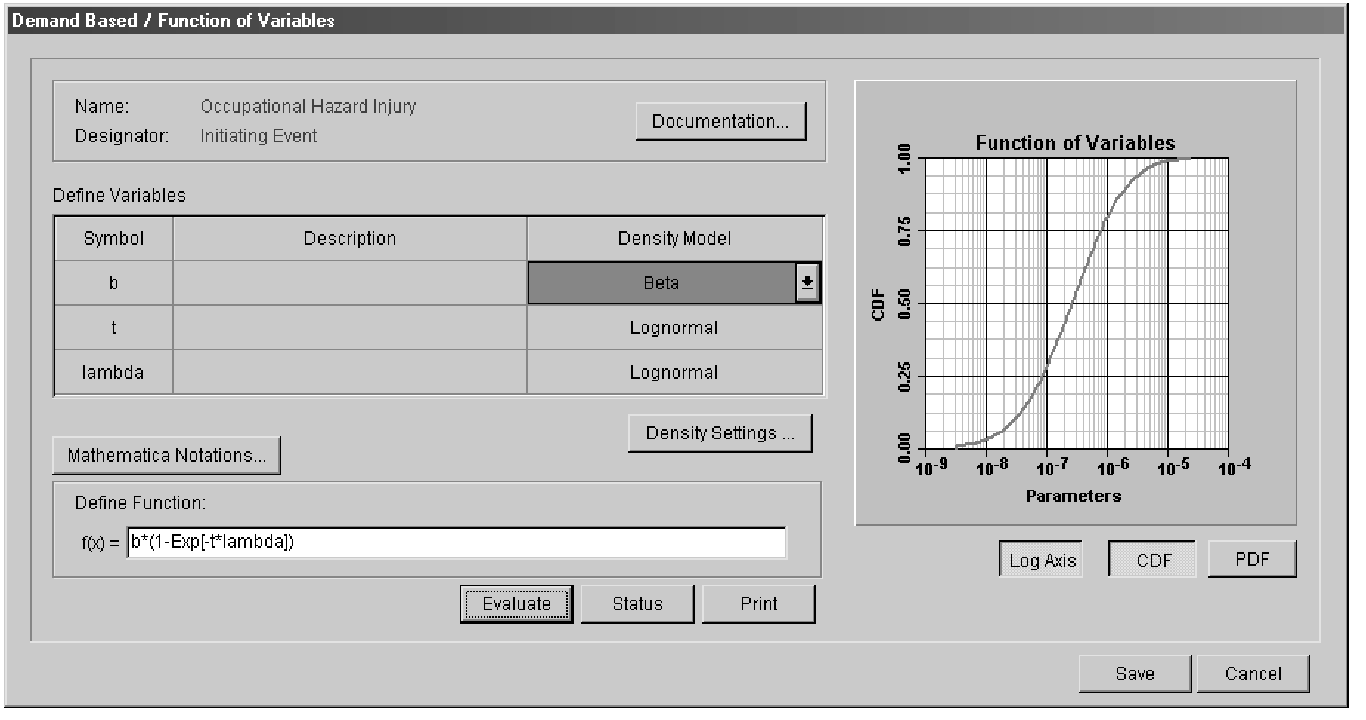
- Uncertainty distributions are used to define the probabilities of events





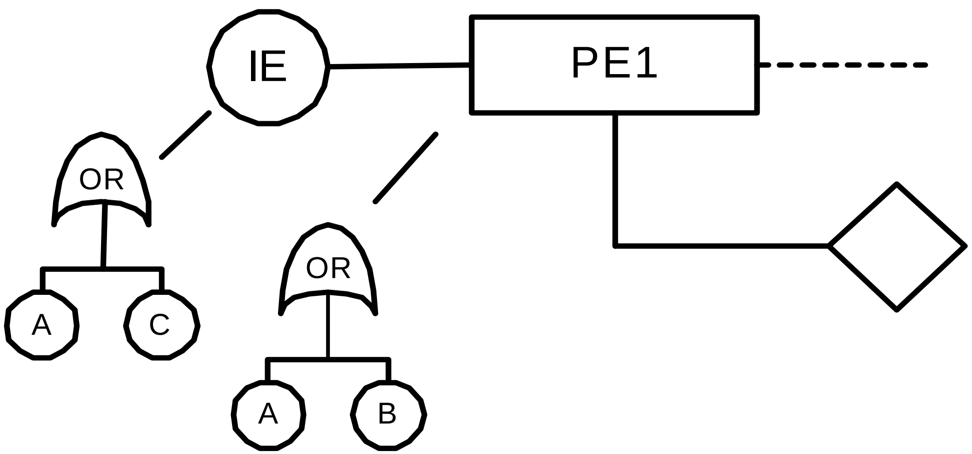
Link with External Tools

- Flexible definition of models through link with Mathematica



Use of Fault Trees for Quantification

Initiating Events and Pivotal Events can be quantified using Fault Trees

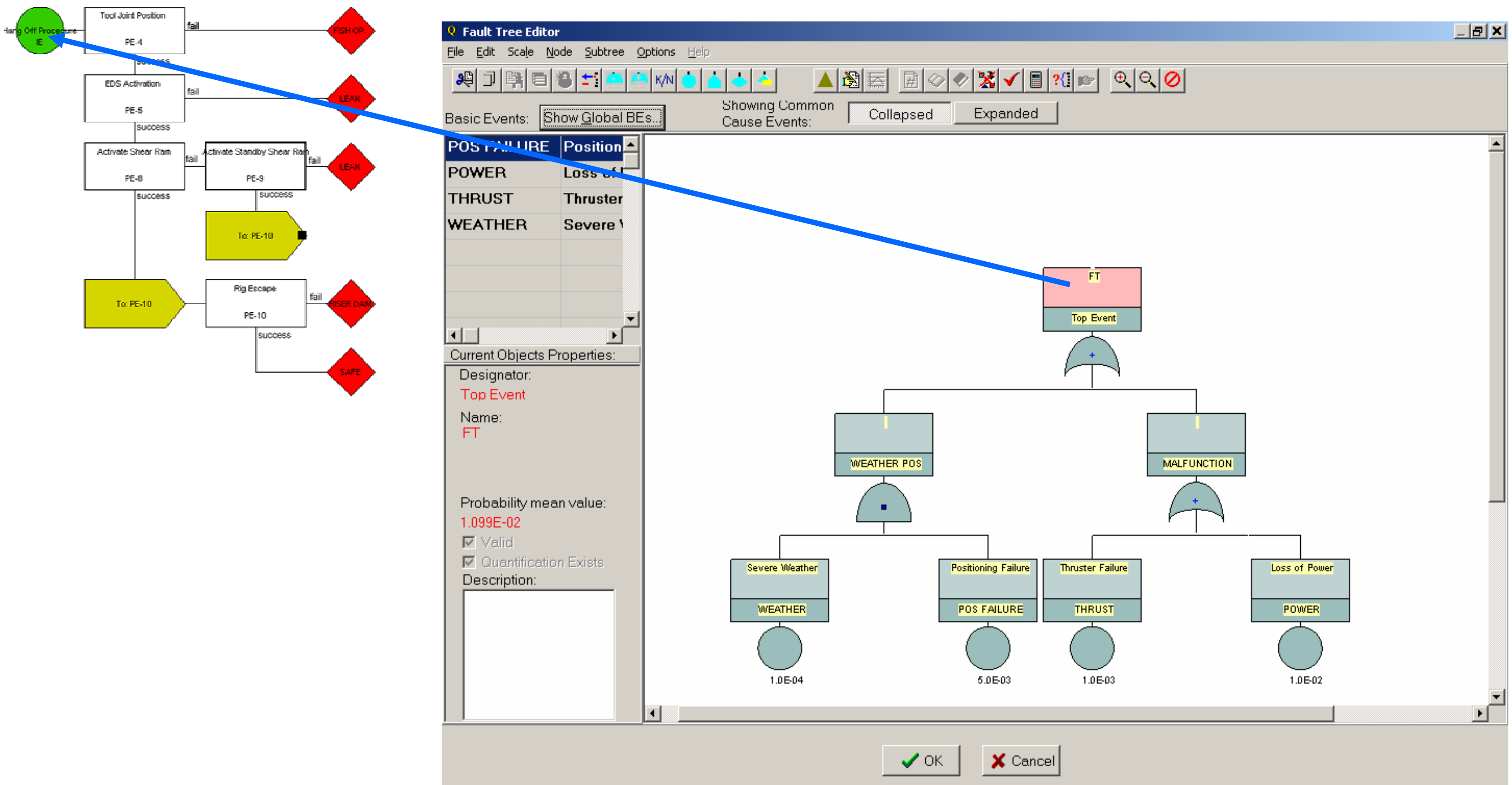


$$\mathrm{IE} \cdot \mathrm{PE1}$$

$$\mathrm{IE} \cdot \overline{\mathrm{PE1}}$$

Adding Detail to ESD Nodes

- Decomposition of events by means of fault trees



Solving and Analyzing Fault Trees

- Fault Trees can be solved for the point estimate probability at any gate level.
- Fault Tree cut sets can be computed at any gate level.
- Fault Tree uncertainty analysis can be performed at the top event level, after solving the top event.

Binary Decision Diagrams in QRAS

- Algorithms to perform analyses have been implemented using Binary Decision Diagram (BDD) techniques
- Cut-sets and event/scenario probabilities are derived from the BDDs
- Now regarded most powerful approach for fault tree analysis

Advantages of BDDs

- BDD-based algorithms offer advantages in terms of accuracy and efficiency:
  - ‘Efficient manipulation of logic’: extremely fast cut-set identification
  - ‘Straightforward treatment of incoherent logic’: consideration of negated fault trees during scenario analysis
  - ‘Exact quantification’: no need to use rare-event type approximations

Size of BDD Encoding of Cut Sets

- There is no strong relationship between number of cuts and the amount of memory to store the BDD-type encoding

- Similarly, no strong relationship between number of cuts and the computation time

Cut-Set Identification in QRAS

- QRAS could possibly identify billions of cuts within seconds
- QRAS guards against attempts to extract too many cuts
  - Constructs the BDD encoding
  - Compares number of cuts against user-specified threshold
  - If below threshold, extracts, sorts, and displays cuts

Truncated Cut-Set Identification

- The search for cut-sets can be limited to significant cuts
- Only identify cuts with specified
  – Maximum order: number of basic events
  – Minimum probability: product of event probabilities
- Takes place during conversion of the BDD

Cut-Set Identification Performance

- Computation time for some real fault trees
  - In seconds, on a 500MHz Pentium 3, 256MB RAM

MAX ORDER	MIN PROB	# CUTS	TIME
-	-	33,983,088	8
6	-	21,802	1
9	-	440,093	13
12	-	3,009,332	300
-	1.00E-12	6,963	1
-	1.00E-18	268,381	18
6	1.00E-12	4,601	1
9	1.00E-18	179237	20

Cut-Set Identification Performance

	MAX ORDER	MIN PROB	# CUTS	TIME
FAULT TREE 2	-	-	>1 billion	1
	4	-	2546	1
	6	-	15,542,373	15
	9	-	-	>1 hour
	-	1.00E-06	12914	1
	-	1.00E-09	880429	7
	-	1.00E-12	13,740,522	150
	4	1.00E-06	0	1
	6	1.00E-12	2,408,779	60
FAULT TREE 3	-	-	4,181,090	1
	6	-	117,394	1
	9	-	1,073,301	2
	12	-	3,013,018	9
	-	1.00E-12	9,088	1
	-	1.00E-18	123,020	1
	6	1.00E-12	8,806	1
	9	1.00E-18	118837	3

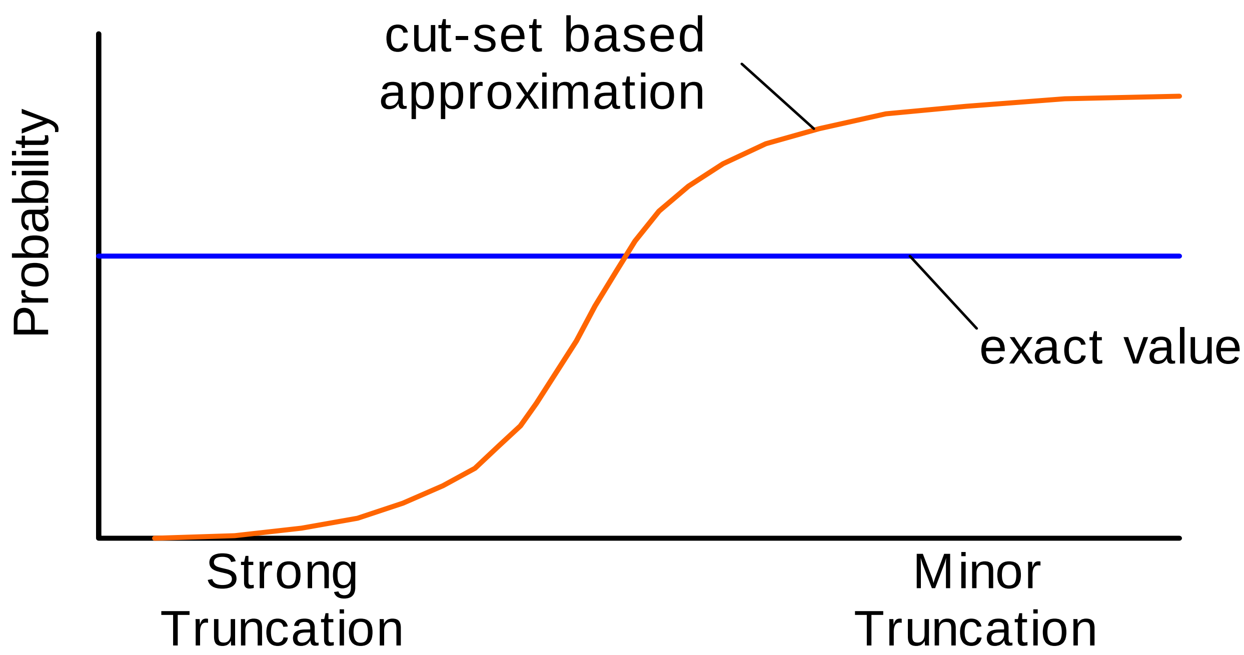
Example: Comparison of Quantification

- Table illustrates varying impact of approximation and truncation in practical cases

	BDD	CUT-SET BASED APPROXIMATION			
		1.00E-08	1.00E-12	1.00E-15	NONE
1	6.53E-08	0.00E+00	6.66E-08	6.71E-08	6.71E-08
2	1.73E-05	1.59E-05	1.94E-05	1.94E-05	1.94E-05
3	3.97E-09	0.00E+00	3.64E-09	5.61E-09	-
4	2.86E-06	1.15E-06	9.66E-06	-	-
5	1.94E-05	2.26E-05	2.29E-06	2.29E-05	-
6	5.94E-07	3.07E-07	1.23E-06	1.25E-06	-
7	5.41E-06	5.76E-06	7.37E-06	7.13E-06	-
8	3.19E-06	3.90E-06	3.90E-06	4.54E-06	-
9	3.48E-10	0.00E+00	3.25E-10	5.29E-10	-
10	4.01E-07	4.50E-07	9.40E-07	9.48E-07	-

Cut-Set Truncation and Quantification

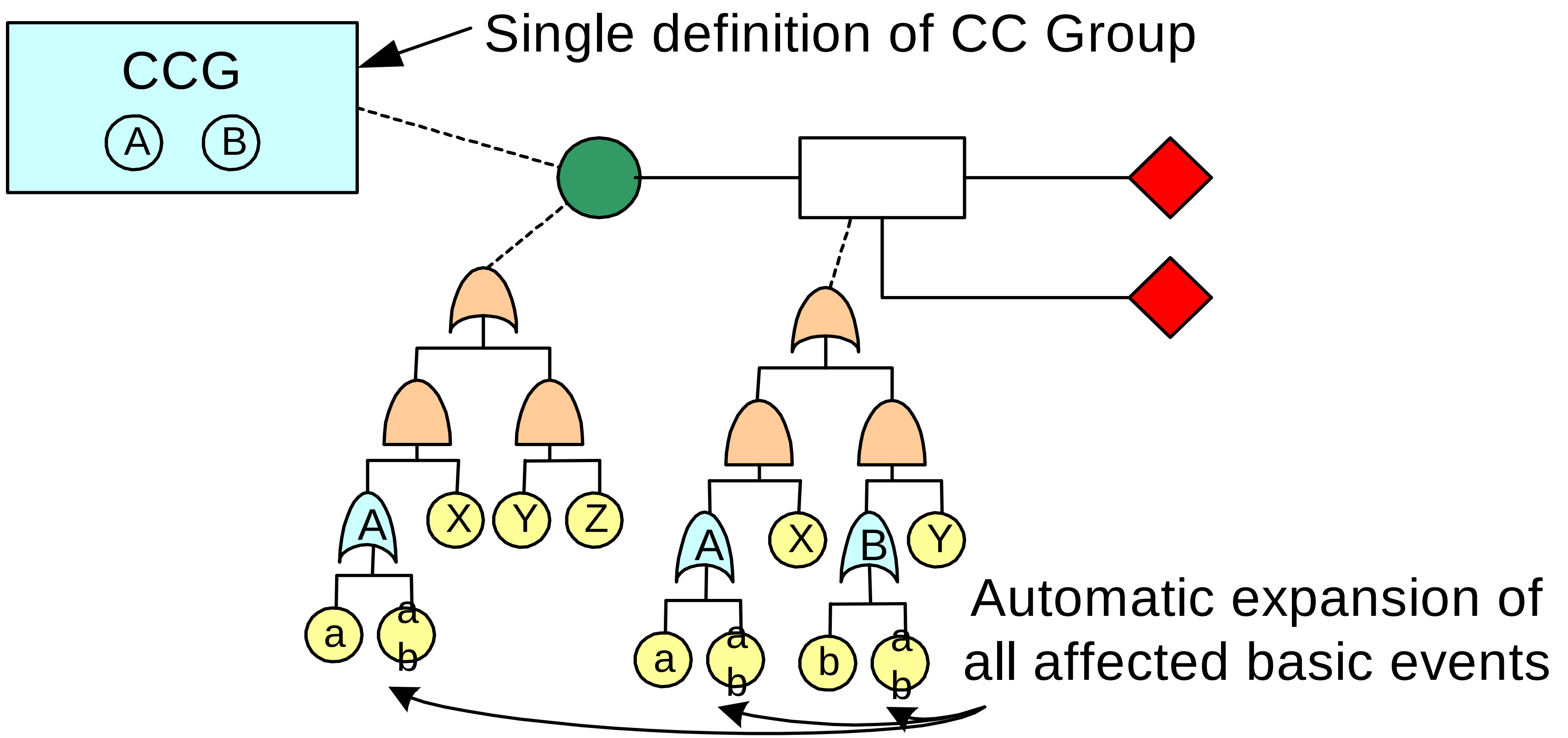
- Truncation during cut-set identification does not affect the quantification
  - Quantification derived directly from BDD



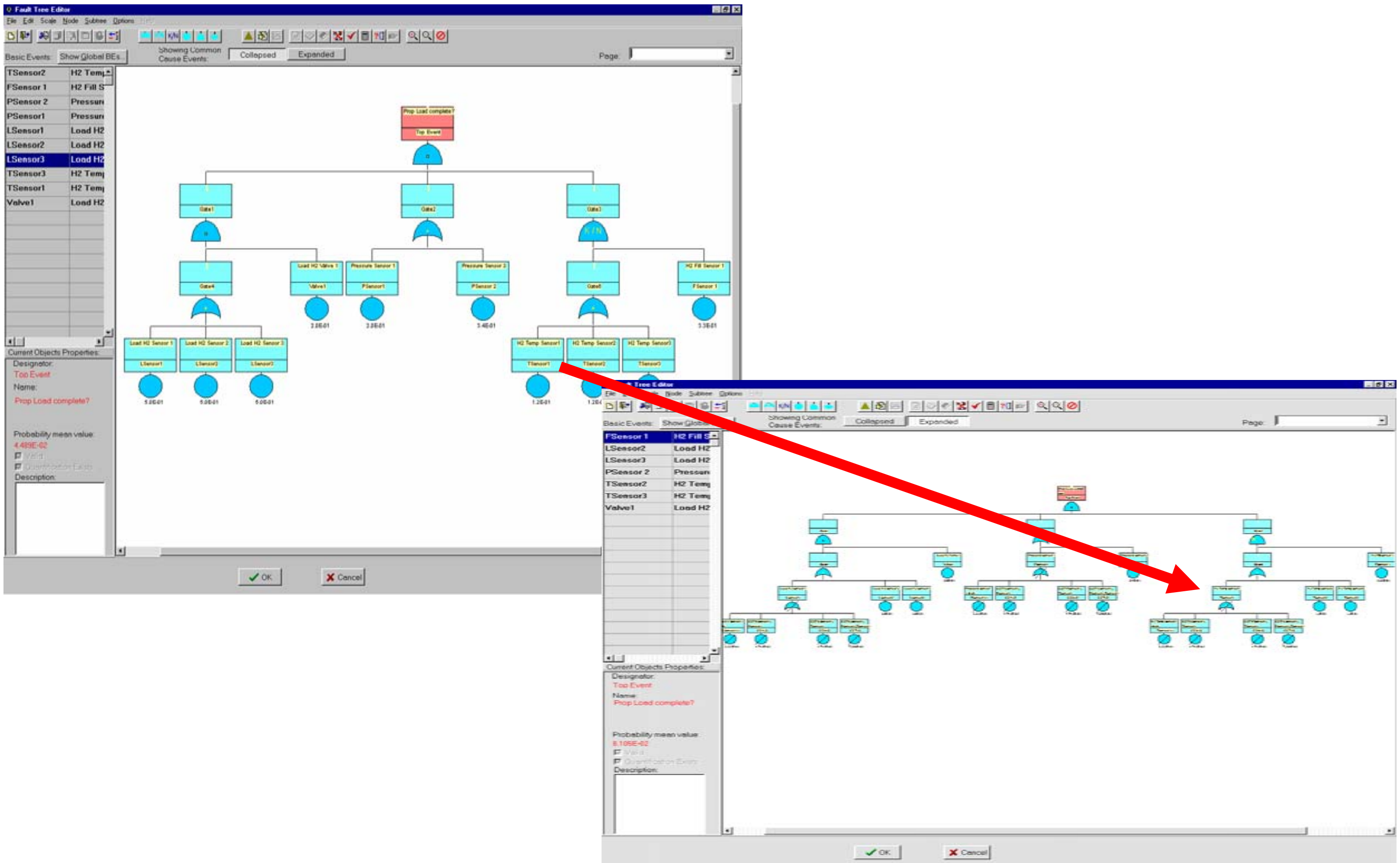
Fault Tree Uncertainty

- Fault Tree Uncertainty Analysis consists of a Monte Carlo procedure in which the BDD probability is repeatedly evaluated
  - Event probabilities sampled from respective distributions
  - Outcomes used to construct distribution

Common Cause Failure Modeling



Common Cause Fault Tree Expansion

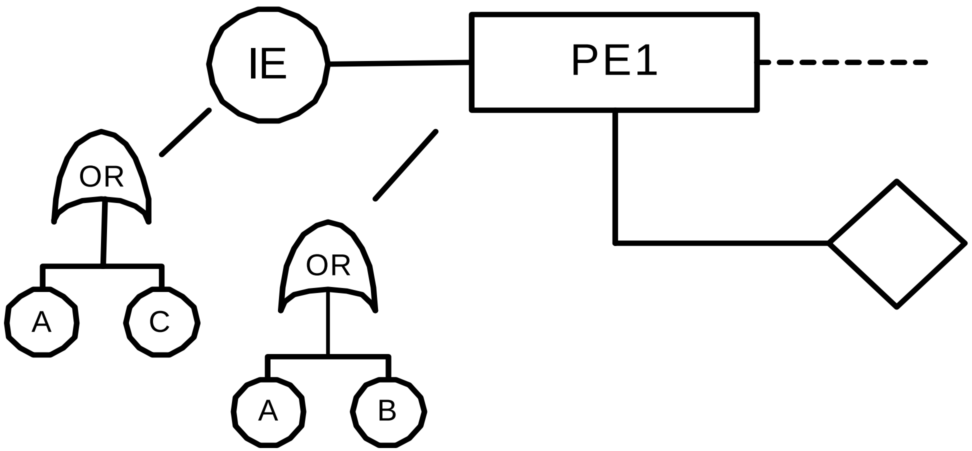


Creating/Running an Analysis

- All standard analyses are run from the **Analysis** top-of-screen menu option. Note that the pull-down menu for **Analysis** contains the following four options:
  - Create Baseline.
  - Create New Analysis.
  - View Prior Analysis Results.
  - Delete Baseline.

Fault Tree Linking

- Fault tree linking is the procedure in which the fault trees in an scenarios are logically combined



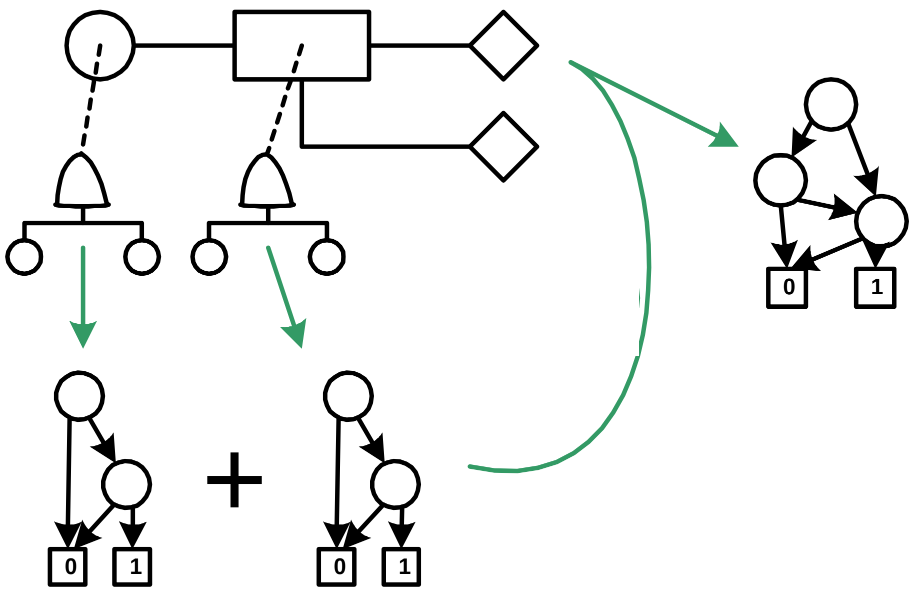
$$IE \cdot PE1$$

$$IE \cdot \overline{PE1}$$

- Outcome is a Boolean function describing conditions under which a scenario is realized

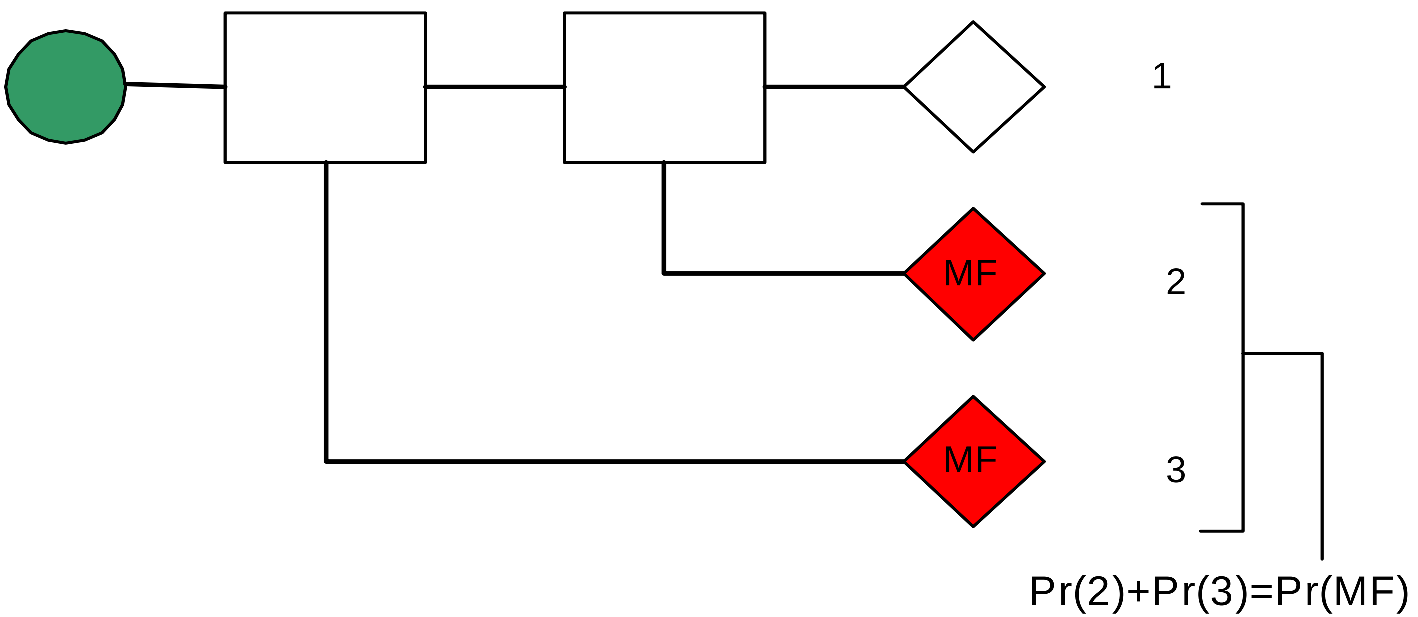
Fault Tree Linking cont…

- Fault tree linking is achieved by combining fault tree BDD according to the logic of the event sequence diagram

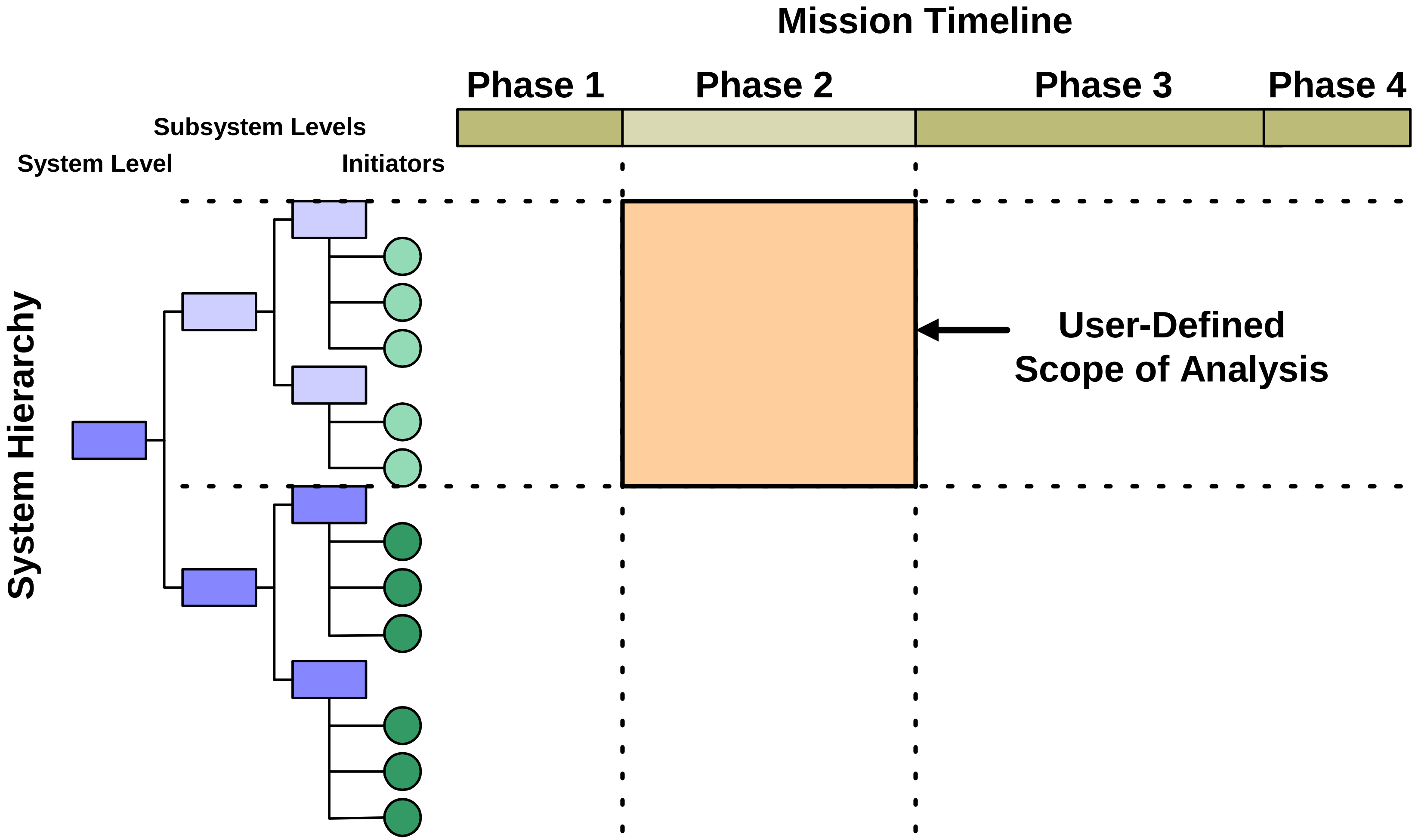


Quantification of End State Types

- Scenarios in an ESD are mutually exclusive
- End state probability found through summation

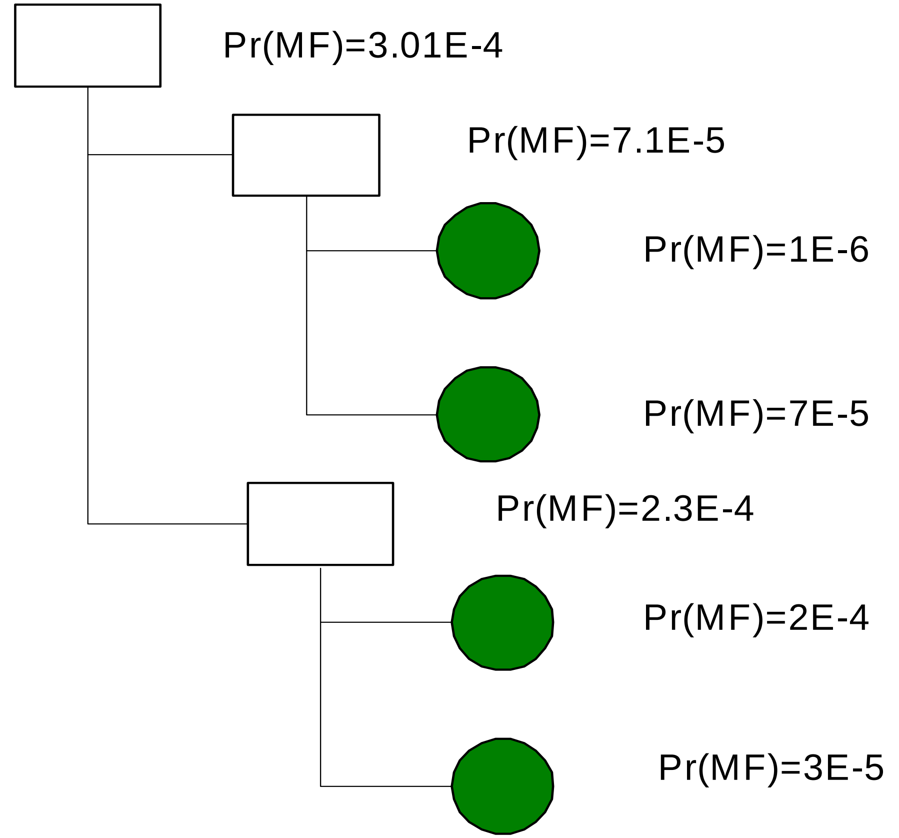


Analysis Scope



Aggregation in System Hierarchy

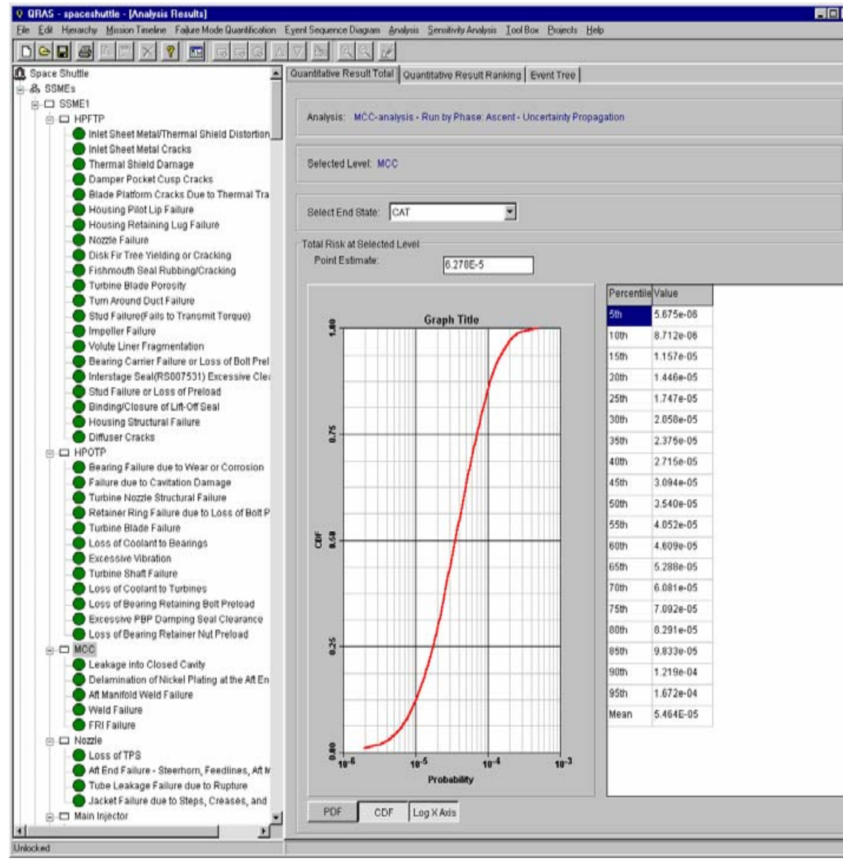
- Summation of probabilities by end state
- Assumption of independence between initiating events



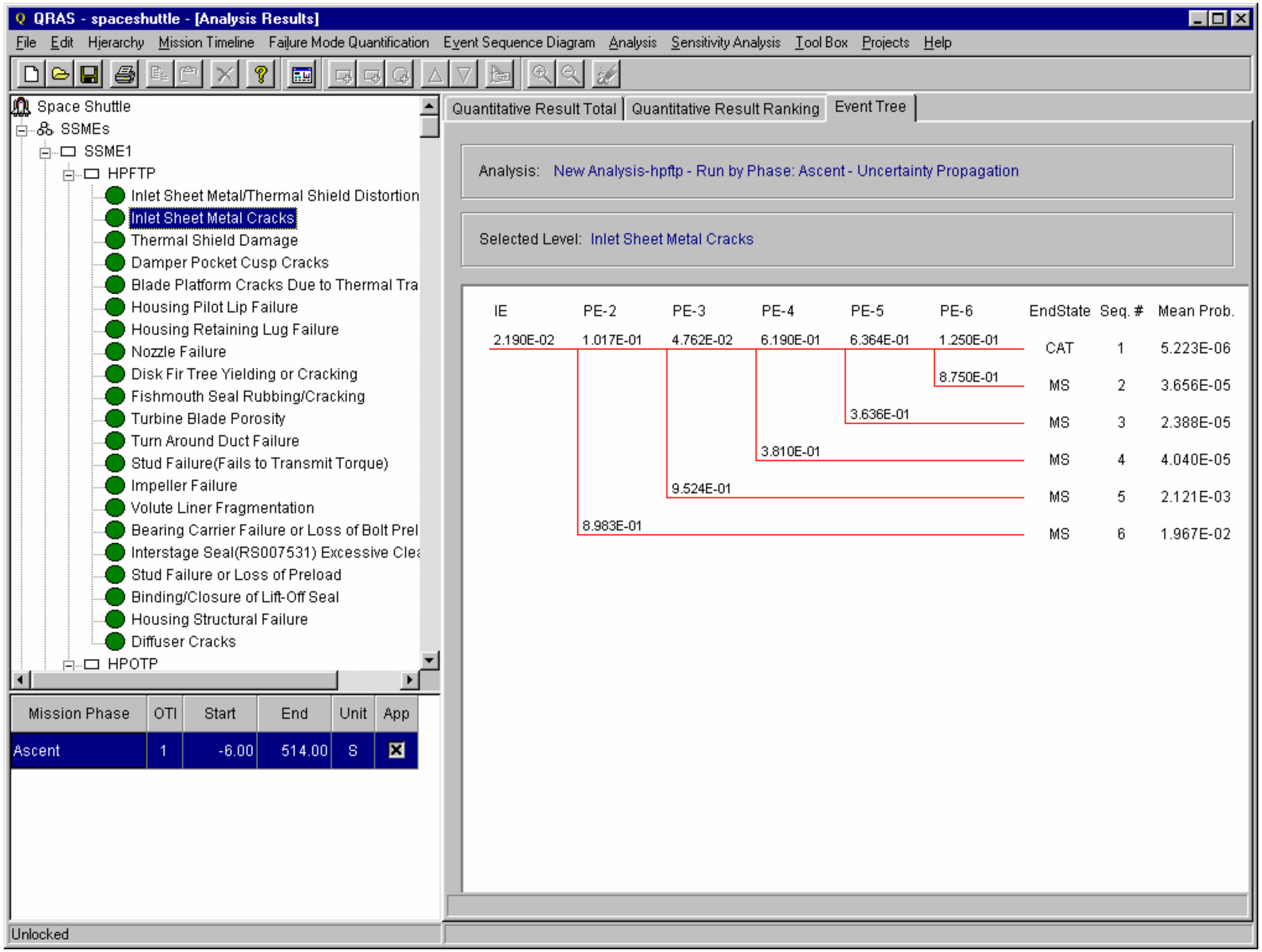
$$\Pr(MF) = \Pr(MF_1) + \Pr(MF_2) - \Pr(MF_1) \cdot \Pr(MF_2)$$

Viewing Aggregation Results

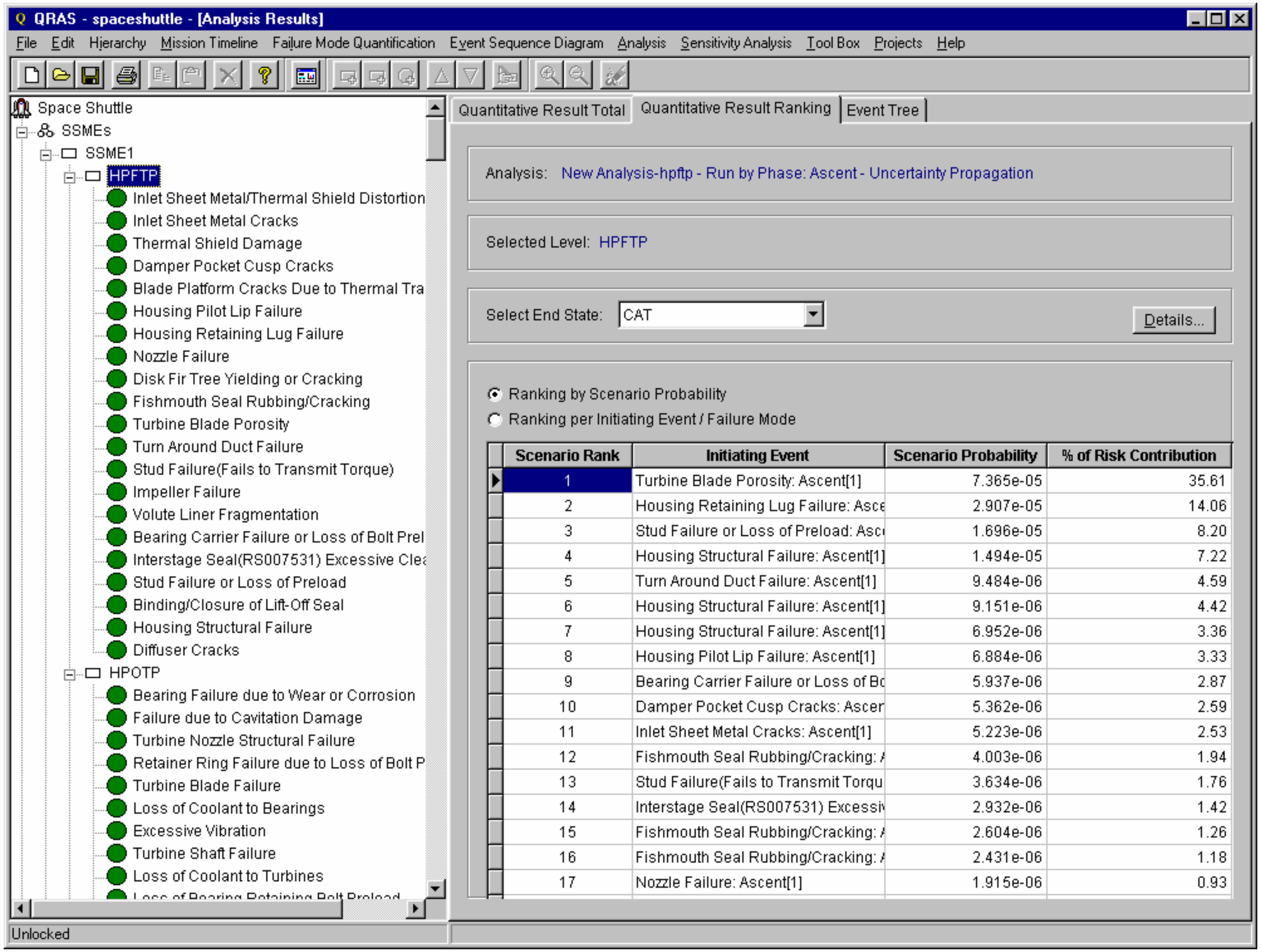
- If the Baseline and Analysis were created for full uncertainty propagation, the end state uncertainty results will be aggregated and shown.



Event Tree

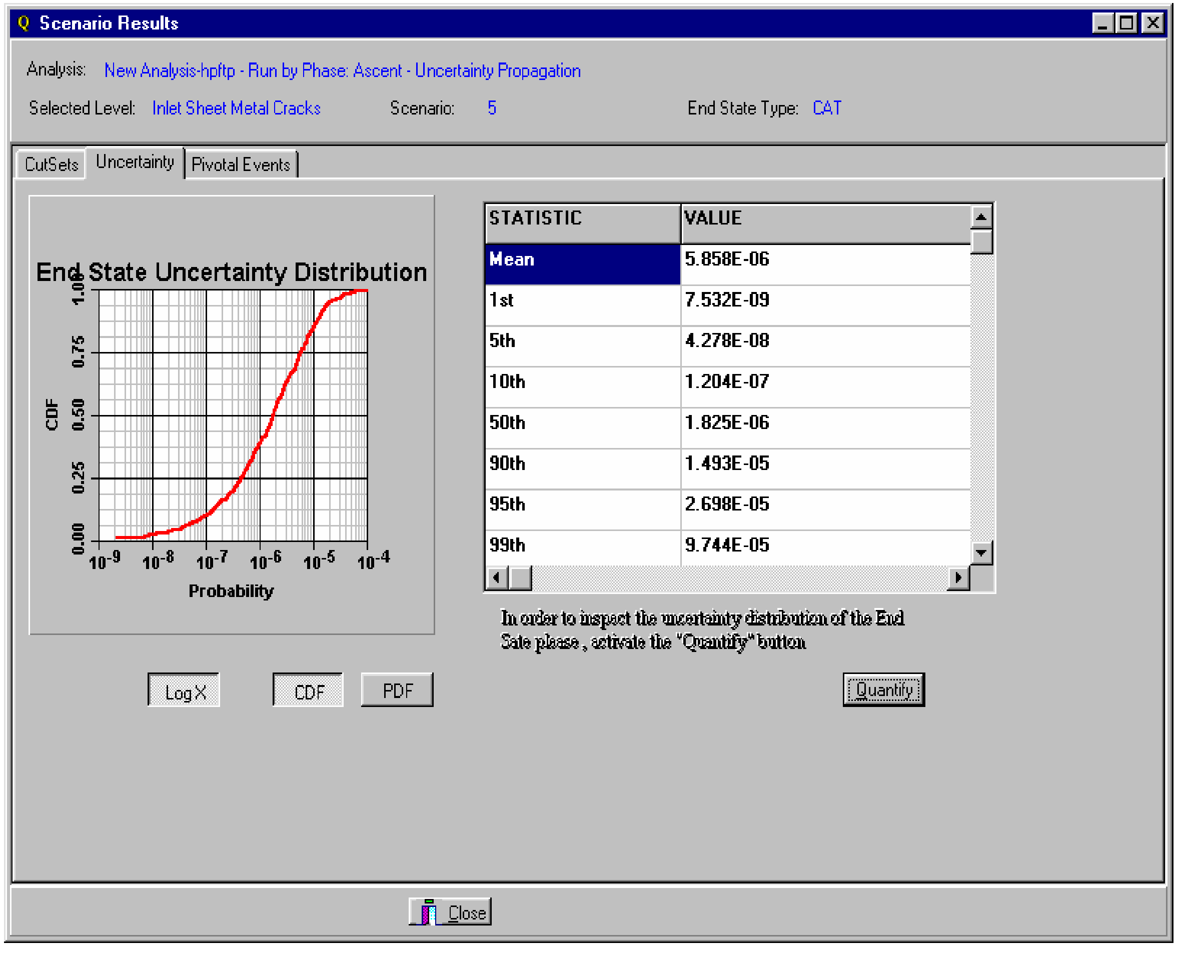

QRAS - spaceshuttle - [Analysis Results]
File Edit Hierarchy Mission Timeline Failure Mode Quantification Event Sequence Diagram Analysis Sensitivity Analysis Tool Box Projects Help
Space Shuttle
SSMEs
SSME1
HPFTP
Inlet Sheet Metal/Thermal Shield Distortion
Inlet Sheet Metal Cracks
Thermal Shield Damage
Damper Pocket Cusp Cracks
Blade Platform Cracks Due to Thermal Tra
Housing Pilot Lip Failure
Housing Retaining Lug Failure
Nozzle Failure
Disk Fir Tree Yielding or Cracking
Fishmouth Seal Rubbing/Cracking
Turbine Blade Porosity
Turn Around Duct Failure
Stud Failure(Fails to Transmit Torque)
Impeller Failure
Volute Liner Fragmentation
Bearing Carrier Failure or Loss of Bolt Prel
Interstage Seal(RS007531) Excessive Clea
Stud Failure or Loss of Preload
Binding/Closure of Lift-Off Seal
Housing Structural Failure
Diffuser Cracks
HPOTP
Mission Phase | OTI | Start | End | Unit | App
Ascent | 1 | -6.00 | 514.00 | S
Unlocked
Quantitative Result Total
Quantitative Result Ranking
Event Tree
Analysis: New Analysis-hpftp - Run by Phase: Ascent - Uncertainty Propagation
Selected Level: Inlet Sheet Metal Cracks
IE PE-2 PE-3 PE-4 PE-5 PE-6 EndState Seq. # Mean Prob.
2.190E-02 1.017E-01 4.762E-02 6.190E-01 6.364E-01 1.250E-01 CAT 1 5.223E-06
8.750E-01 MS 2 3.656E-05
3.636E-01 MS 3 2.388E-05
3.810E-01 MS 4 4.040E-05
9.524E-01 MS 5 2.121E-03
8.983E-01 MS 6 1.967E-02

Viewing Results Ranking



Scenario Rank	Initiating Event	Scenario Probability	% of Risk Contribution
1	Turbine Blade Porosity: Ascent[1]	7.365e-05	35.61
2	Housing Retaining Lug Failure: Asce	2.907e-05	14.06
3	Stud Failure or Loss of Preload: Asc	1.696e-05	8.20
4	Housing Structural Failure: Ascent[1]	1.494e-05	7.22
5	Turn Around Duct Failure: Ascent[1]	9.484e-06	4.59
6	Housing Structural Failure: Ascent[1]	9.151e-06	4.42
7	Housing Structural Failure: Ascent[1]	6.952e-06	3.36
8	Housing Pilot Lip Failure: Ascent[1]	6.884e-06	3.33
9	Bearing Carrier Failure or Loss of Bc	5.937e-06	2.87
10	Damper Pocket Cusp Cracks: Ascer	5.362e-06	2.59
11	Inlet Sheet Metal Cracks: Ascent[1]	5.223e-06	2.53
12	Fishmouth Seal Rubbing/Cracking: /	4.003e-06	1.94
13	Stud Failure(Fails to Transmit Torqu	3.634e-06	1.76
14	Interstage Seal(RS007531) Excessiv	2.932e-06	1.42
15	Fishmouth Seal Rubbing/Cracking: /	2.604e-06	1.26
16	Fishmouth Seal Rubbing/Cracking: /	2.431e-06	1.18
17	Nozzle Failure: Ascent[1]	1.915e-06	0.93

Viewing Scenario Details



Sensitivity Analysis

- A sensitivity analysis, also called a "what if" analysis, allows the user to:
  - Change quantifications of failure modes or ESD pivotal events.
  - Remove failure modes or subsystems.
  - Add failure modes or entire subsystems.

- The sensitivity analysis changes are not permanently stored.

Sensitivity Analysis Results Screen